Amendments to the Specification:

Please amend the specification as indicated at the bracketed paragraph numbers below:

[0035] Figure 2 illustrates the operation of the verification engine in an authentication system provided for authenticating a subject in an electronic commerce transaction. In this context, the subject is labeled the "Customer," the authentication client is the "e-commerce site," the independent databases are the "trusted Validator (boxes 3a, 3b, etc.)," (*e.g.*, Bank, Credit Bureau, etc.) and the verification engine is being operated by the "Authentex" entity. For simplicity in Figure 2, the queries and response paths are illustrated as going directly to the verification engine, rather than through the authentication client. Figure 2 illustrates both "real-time interactions" (*e.g.*, in-wallet and out-of-wallet queries (box 8), query responses (box 9), appropriate out-of-wallet data queries (box 6), match confidences (box 7), in-wallet query responses (box 12), match confidences (box 13), and authentication confidence (box 14)) and "non real-time interactions" (*e.g.*, negotiating the allowed queries (box 5), physical validation (box 2), and collecting out-of-wallet data (box 4)). However, any of the interactions may be either "real-time" or "non real-time."

[0036] With reference to Figure 2, the Customer (box 1) logs onto an e-commerce site (box 15) for which Authentex (box 10) provides authentication. The system will ask the Customer a series of appropriate questions (box 8) to authenticate his identity. These questions center on in-wallet data that Authentex itself possesses, and out-of-wallet data possessed by a trusted Validator (boxes 3a, 3b, etc.) such as a bank or credit bureau. Authentex holds in-wallet data and provides the gateway to Validators who hold out-of-wallet data.

[0037] The questions are "appropriate" in that they fit the situation. Clearly asking for name, address, phone number, and Social Security Number would be seeking appropriate in-wallet data that can be used to authenticate the Customer. Choosing appropriate out-of-wallet questions is more difficult. Out-of-wallet data (box 4) and physical validation (*e.g.*, Passport, Drivers License, Birth Certificate, etc.) of the Customer (box 2) were collected by the Validator through the course of its normal interactions with the Customer, independent of any connection with Authentex. For example, the Trusted Validator (box

3) and the Customer (box 1) establish face-to-face interaction when the Customer opens a bank account. Out-of-wallet data is generated at each subsequent truncation with the Customer. The Validators build up a database of information, and a series of queries that can be put to that database. Authentex and the Validator establish a set of allowed queries (box 5) which is a subset of all the queries permitted by the Validator's database, chosen to provide proper authentication while being as unobtrusive as possible. Effectively, the Validator is digitally vouching for the Customer.

Please add the following new paragraphs to the specification:

[0020a] Figure 3 is a flow chart illustrating a method of user authentication according to one embodiment.

[0039a] Figure 3 is a flow chart illustrating a method 300 of user authentication according to one embodiment. At step 305, one or more allowed queries are negotiated with one or more independent, third-party databases. For example, as shown in Figure 2, Authentex (box 10) and Trusted Validator (box 3) agree on queries that can be asked on the Trusted Validator's system. At step 310, one or more of the allowed queries are presented to the subject. For example, with reference to Figure 2, Authentex (box 10) can ask the Customer (box 1) for appropriate in-wallet and appropriate out-of-wallet information. At step 315, answers to the one or more queries are received from the subject.

[0039b] At step 320, the one or more allowed queries and/or the one or more received answers are presented to the independent, third-party databases. For example, with reference to Figure 2, Authentex (box 10) can check the out-of-wallet data with the Trusted Validator (box 3). At step 325, match confidences are received from the independent, third-party databases. For example, after being asked an allowed query, the database may respond with a yes or no answer and the confidence the database has in that answer. At step 330, an overall authentication confidence is determined. As shown in Figure 2, Authentex (box 10) assembles answers, determines an overall confidence (box 14) and passes on the overall confidence to the E-Commerce Site (box 15), which can make the final authentication decision.